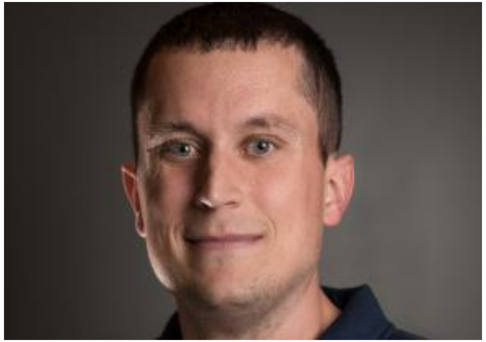
Utilizing operations data for enhanced cyber threat detection and response in industrial control systems (ICS).

Mark Johnson-Barbier & Dan Gunter

Delivering water and power®

About

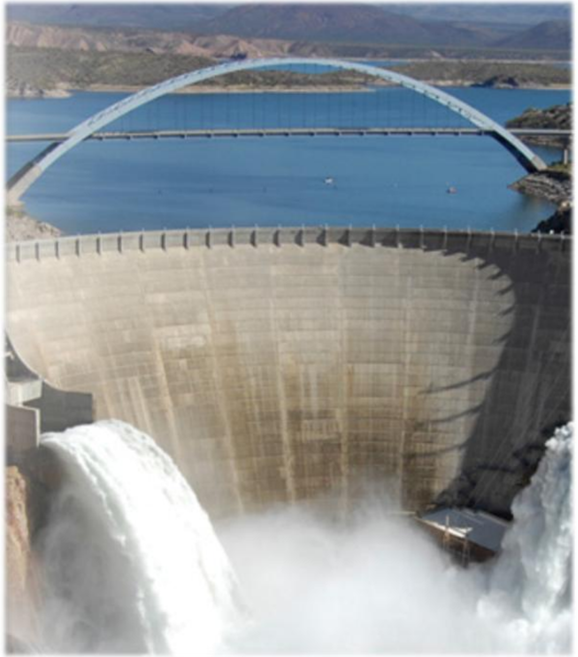


- Dan Gunter
- Principal Threat Analyst
- Dragos
- @dan_gunter

- Mark Johnson-Barbier
- Sr. Principal Analyst
- Salt River Project
- @PulseOut101

About SRP

- Founded 1903 (10 Years before AZ statehood): First multipurpose project under the National Reclamation act of 1902
  - 5089 employees
  - 1,041,342 customers
  - 2,900 sq mile service area
  - 375 sq mile water service area
  - 13,000 sq mile watershed
- Salt River Valley Water Users' Association
  - 10 member board and 30 member council – elected by landowners
  - Canals largely follow 500 miles of ditches built 400-1450AD by the Hohokam
  - 2018 Water delivery: 773,527 acre-feet
  - 8 dams and lakes
- Salt River Project Agricultural Improvement and Power District
  - 14 member board and 30 member council – elected by landowners
  - Generation Owner/Operator: 1 Nuclear, 12 Fossil, 8 hydro plants
  - Generation: Biomass, Utility Solar, Wind, Geothermal, Rooftop Solar
  - Transmission & Distribution
  - Peak Power System: 7,610 MW
  - Sustainable Portfolio 17.25% of retail requirements

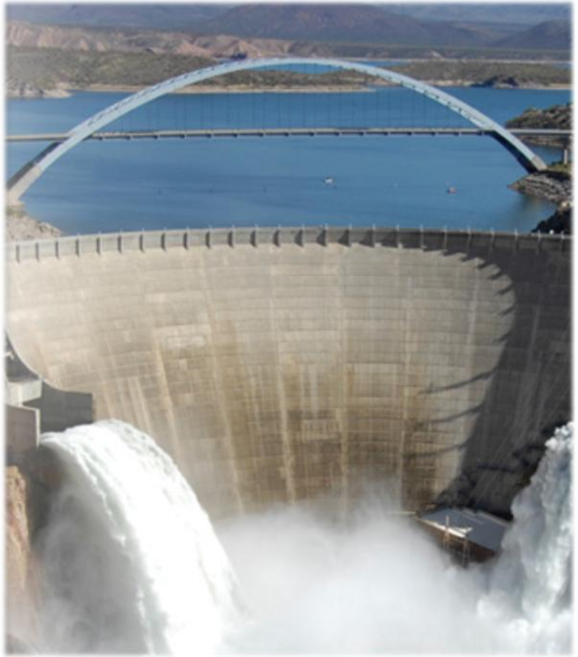


About SRP

- Founded 1903 (10 Years before AZ statehood): First multipurpose project under the National Reclamation act of 1902
  - 5089 employees
  - 1,041,342 customers
  - 2,900 sq mile service area
  - 375 sq mile water service area
  - 13,000 sq mile watershed

= .05 Texas

- Salt River Valley Water Users' Association
  - 10 member board and 30 member council – elected by landowners
  - Canals largely follow 500 miles of ditches built 400-1450AD by the Hohokam
  - 2018 Water delivery: 773,527 acre-feet
  - 8 dams and lakes
- Salt River Project Agricultural Improvement and Power District
  - 14 member board and 30 member council – elected by landowners
  - Generation Owner/Operator: 1 Nuclear, 12 Fossil, 8 hydro plants
  - Generation: Biomass, Utility Solar, Wind, Geothermal, Rooftop Solar
  - Transmission & Distribution
  - Peak Power System: 7,610 MW
  - Sustainable Portfolio 17.25% of retail requirements

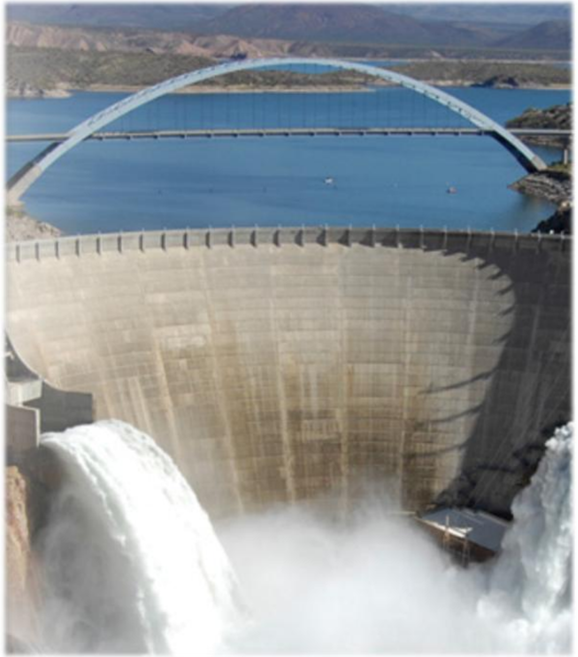


About SRP

- Founded 1903 (10 Years before AZ statehood): First multipurpose project under the National Reclamation act of 1902
  - 5089 employees
  - 1,041,342 customers
  - 2,900 sq mile service area
  - 375 sq mile water service area
  - 13,000 sq mile watershed

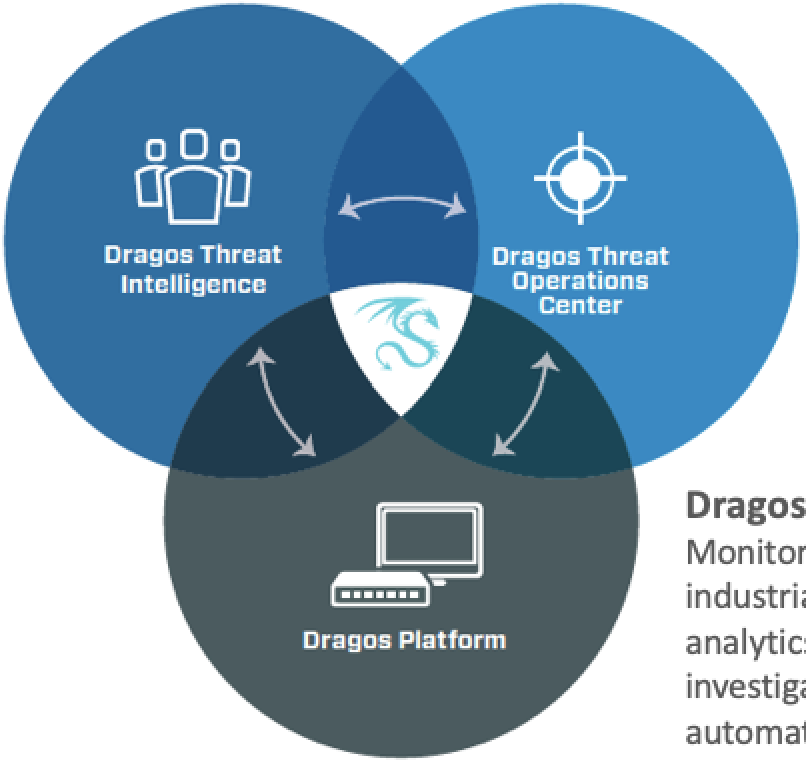
= .021043125 QLD

- Salt River Valley Water Users' Association
  - 10 member board and 30 member council – elected by landowners
  - Canals largely follow 500 miles of ditches built 400-1450AD by the Hohokam
  - 2018 Water delivery: 773,527 acre-feet
  - 8 dams and lakes
- Salt River Project Agricultural Improvement and Power District
  - 14 member board and 30 member council – elected by landowners
  - Generation Owner/Operator: 1 Nuclear, 12 Fossil, 8 hydro plants
  - Generation: Biomass, Utility Solar, Wind, Geothermal, Rooftop Solar
  - Transmission & Distribution
  - Peak Power System: 7,610 MW
  - Sustainable Portfolio 17.25% of retail requirements



About Dragos

Dragos WorldView
Expertise and knowledge in ICS threat identification and understanding delivered in weekly reports and briefings



Dragos ThreatView
Experienced ICS Threat Hunting, Incident Response, and Training delivered as a service

Dragos Platform
Monitoring system that passively identifies industrial assets, utilizes threat behavior analytics to identify threats, and offers investigation playbooks and workflow automation for Incident Response

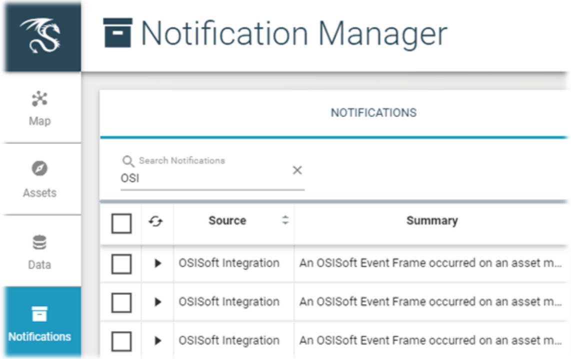
Agenda

- 3 Business/Security Challenges
- Integration of PI System and Threat Detection assists with these challenges
- SRP Test implementation (Proof of Concept)
- Solution, Plans, Ideas for future use cases

3 Business/Security Challenges

SRP

Enhance Cyber Threat detection with PI data



Notification Manager

NOTIFICATIONS

Search Notifications: OSI

□		Source	Summary
□	▸	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...
□	▸	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...
□	▸	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...

CHALLENGE

1. Eliminate threat activity as direct cause of operational outages
2. Improve detection of adversary tradecraft targeting OT
3. Provide data supporting fast & accurate Incident Response

SOLUTION

Integrate PI data with the Threat detection platform

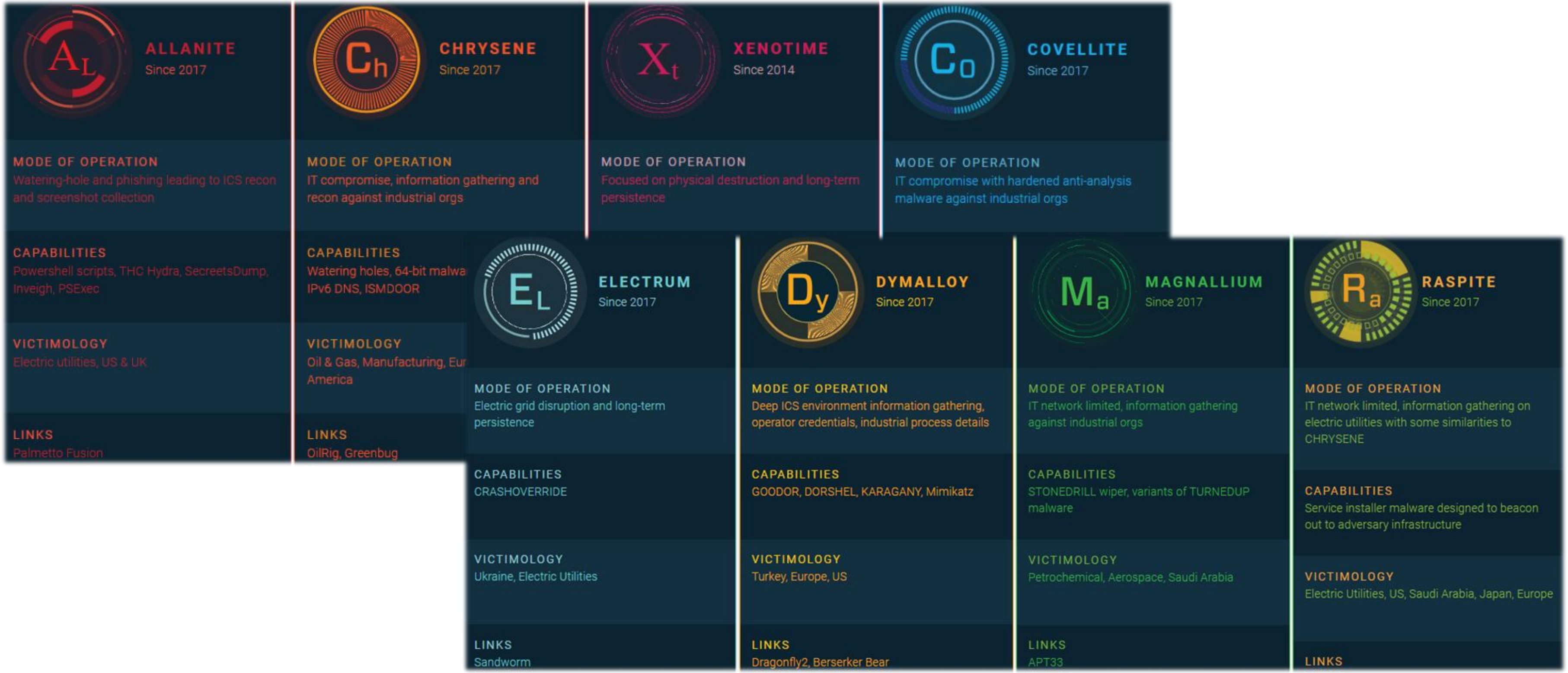
- PI Event Frames notify on specific events
- Dragos Platform correlates PI data with network and endpoint data

RESULTS

Business Challenge: Eliminate Threat activity as cause of operational upsets

- July 2004 Substation Fire
  - High temps: 111°F/44°C
  - Avg Temps: 101°F/38°C
- Sep 8 2011 San Diego
- July 2018 Transformer bushing

Business Challenge: Preventing Breach



ALLANITE
Since 2017

MODE OF OPERATION
Watering-hole and phishing leading to ICS recon and screenshot collection

CAPABILITIES
Powershell scripts, THC Hydra, SecreetsDump, Inveigh, PSExec

VICTIMOLOGY
Electric utilities, US & UK

LINKS
Palmetto Fusion

CHRYSENE
Since 2017

MODE OF OPERATION
IT compromise, information gathering and recon against industrial orgs

CAPABILITIES
Watering holes, 64-bit malwa
IPv6 DNS, ISMDOOR

VICTIMOLOGY
Oil & Gas, Manufacturing, Eur
America

LINKS
OilRig, Greenbug

XENOTIME
Since 2014

MODE OF OPERATION
Focused on physical destruction and long-term persistence

COVELLITE
Since 2017

MODE OF OPERATION
IT compromise with hardened anti-analysis malware against industrial orgs

ELECTRUM
Since 2017

MODE OF OPERATION
Electric grid disruption and long-term persistence

CAPABILITIES
CRASHOVERRIDE

VICTIMOLOGY
Ukraine, Electric Utilities

LINKS
Sandworm

DYMALLOY
Since 2017

MODE OF OPERATION
Deep ICS environment information gathering, operator credentials, industrial process details

CAPABILITIES
GOODOR, DORSHEL, KARAGANY, Mimikatz

VICTIMOLOGY
Turkey, Europe, US

LINKS
Dragonfly2, Berserker Bear

MAGNALLIUM
Since 2017

MODE OF OPERATION
IT network limited, information gathering against industrial orgs

CAPABILITIES
STONEDRILL wiper, variants of TURNEDUP malware

VICTIMOLOGY
Petrochemical, Aerospace, Saudi Arabia

LINKS
APT33

RASPITE
Since 2017

MODE OF OPERATION
IT network limited, information gathering on electric utilities with some similarities to CHRYSENE

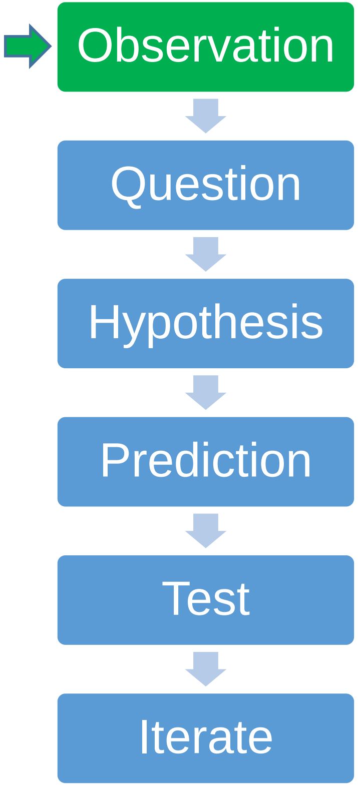
CAPABILITIES
Service installer malware designed to beacon out to adversary infrastructure

VICTIMOLOGY
Electric Utilities, US, Saudi Arabia, Japan, Europe

LINKS

Business Challenge: Incident Response

Well, the resolution's too poor.
It won't help much to enhance it.
FBI



Observation

Question

Hypothesis

Prediction

Test

Iterate

ICS Events

- German Steel Mill
- Trisis
- Crashoverride (Ukraine 2016) Event
- Ukraine 2015

2015 Ukraine Attack Summary

3
Utilities Attacked

225 K
Customer Outages

3.5 hr
Outage Duration.

135 MW
Load impact

100’s
Server and Workstation Damage

10’s
Field Device Damage

50
Substations Impacted

2016 Ukraine Attack Summary

1

Trans Co. Attacked

TBD

Customer Outages

1.25 hr

Outage Duration.

200 MW

Load impact

TBD

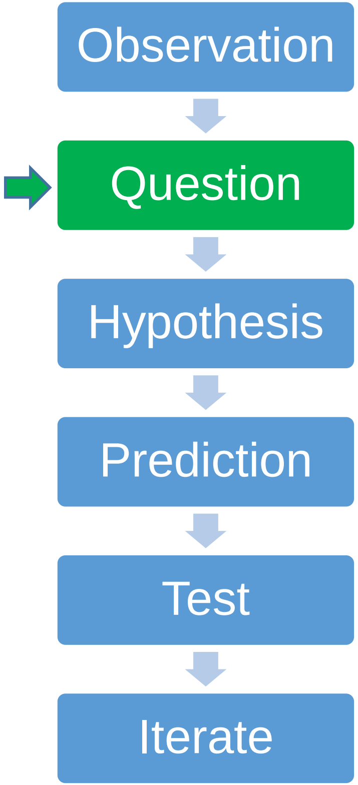
Server and Workstation Damage

TBD

Field Device Damage

1

Substation(s) Impacted



Observation

Question

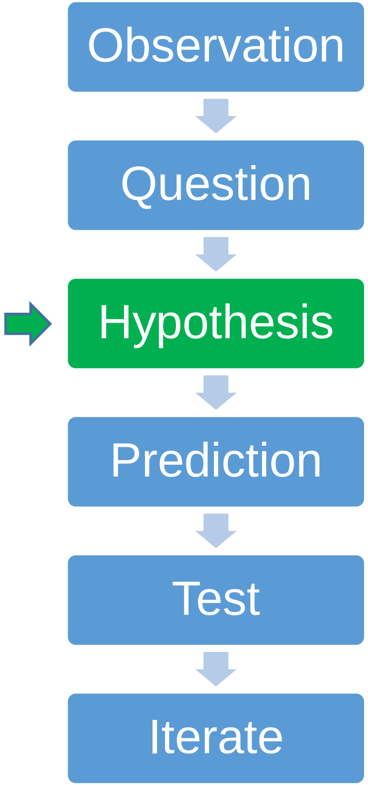
Hypothesis

Prediction

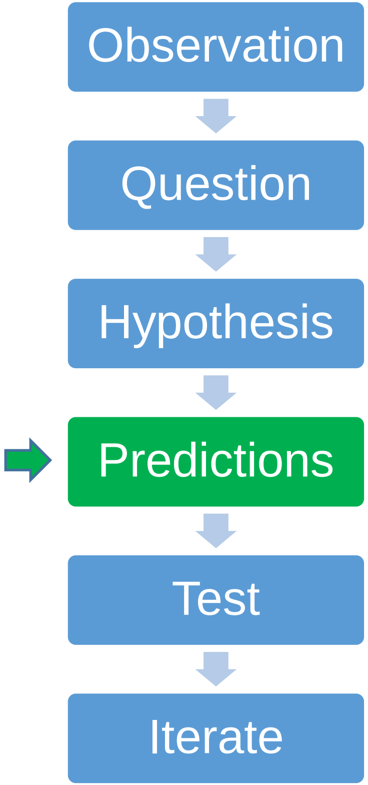
Test

Iterate

How can we prevent, detect, and respond to a cyber attack at SRP?



Adversary will utilize similar tactics as Electrum during an intrusion and will attempt to open breakers from the EMS system



Observation

Question

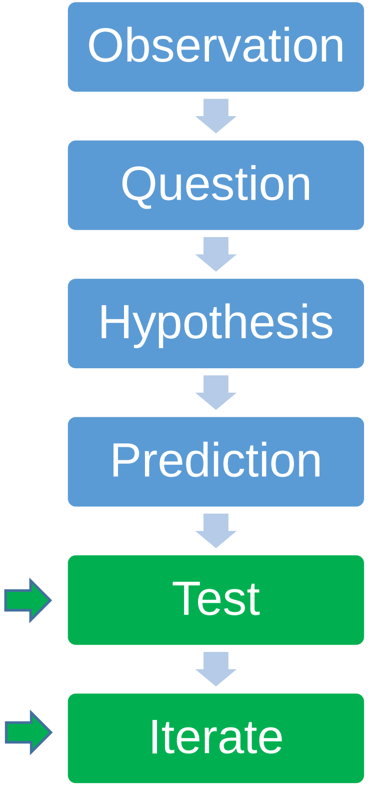
Hypothesis

Predictions

Test

Iterate

1. If prevention fails, SRP can detect an adversary who opens a breaker by sending DNP3 operate commands from an abnormal source computer
2. SOC analysts will quickly gather data to prove or disprove cyber attack as the cause of disruption



Observation

Question

Hypothesis

Prediction

Test

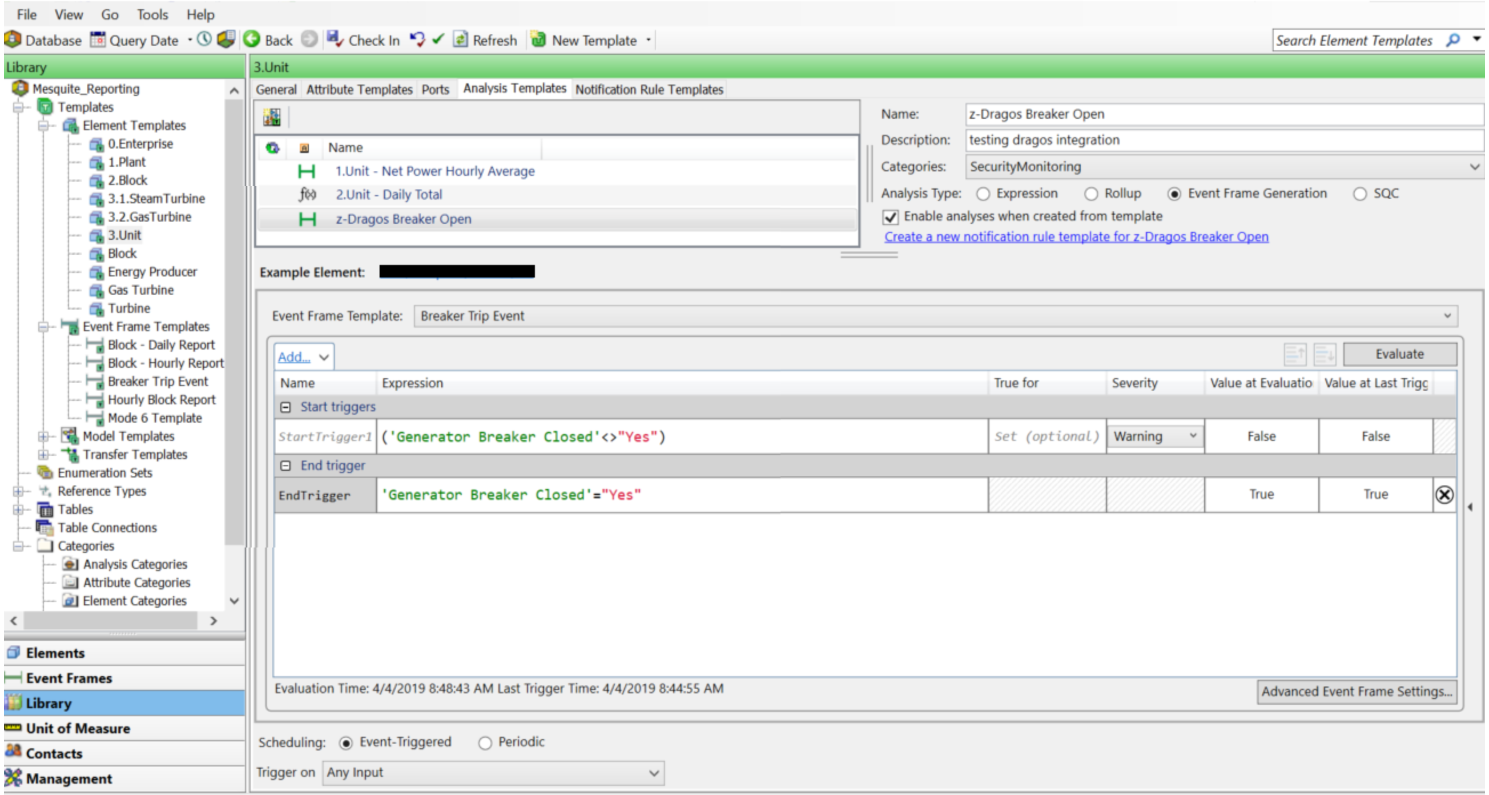
Iterate

Test: Prevent, Detect, Respond to adversary using	Result
Existing corporate controls	• Prevent: most, but not all, adversaries • Detect: untargeted att&cks • Respond: Slow
Add Threat Focused network monitoring platform	• Prevent: adds active defense capability to prevent att&ck techniques • Detect: targeted att&cks • Respond: Med
Integrate data from PI system	• Respond: Expect Fast but TBD

Integrating: PI + Dragos

Test

Event Frame on breaker open event



Name
1.Unit - Net Power Hourly Average
2.Unit - Daily Total
z-Dragos Breaker Open

Name: z-Dragos Breaker Open

Description: testing dragos integration

Categories: SecurityMonitoring

Analysis Type: ○ Expression ○ Rollup ● Event Frame Generation ○ SQC

☑ Enable analyses when created from template

Create a new notification rule template for z-Dragos Breaker Open

Example Element: [redacted]

Event Frame Template: Breaker Trip Event

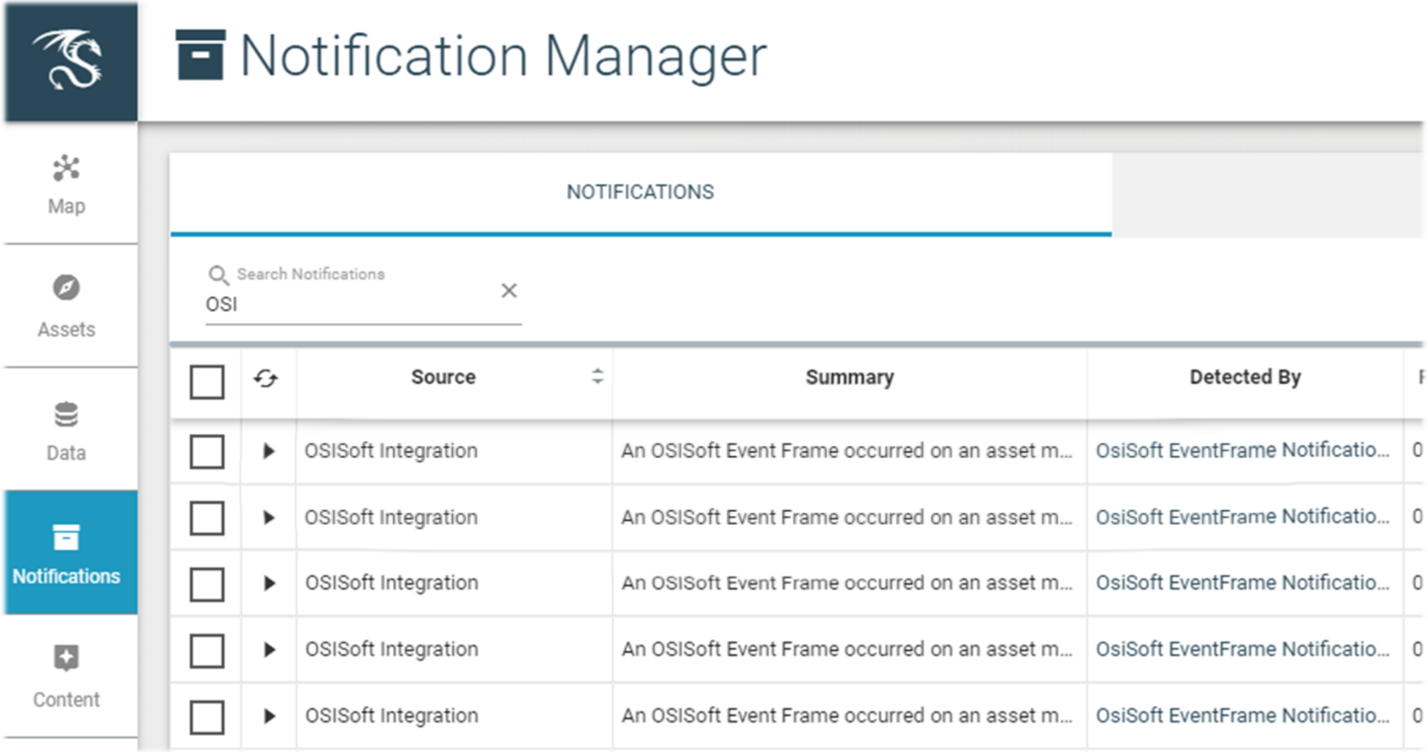
Name	Expression	True for	Severity	Value at Evaluatio	Value at Last Trigg
⊟ Start triggers					
StartTrigger1	('Generator Breaker Closed'<>"Yes")	Set (optional)	Warning	False	False
⊟ End trigger					
EndTrigger	'Generator Breaker Closed'="Yes"			True	True

Evaluation Time: 4/4/2019 8:48:43 AM Last Trigger Time: 4/4/2019 8:44:55 AM

Scheduling: ● Event-Triggered ○ Periodic

Trigger on Any Input

Test Notification



Notification Manager

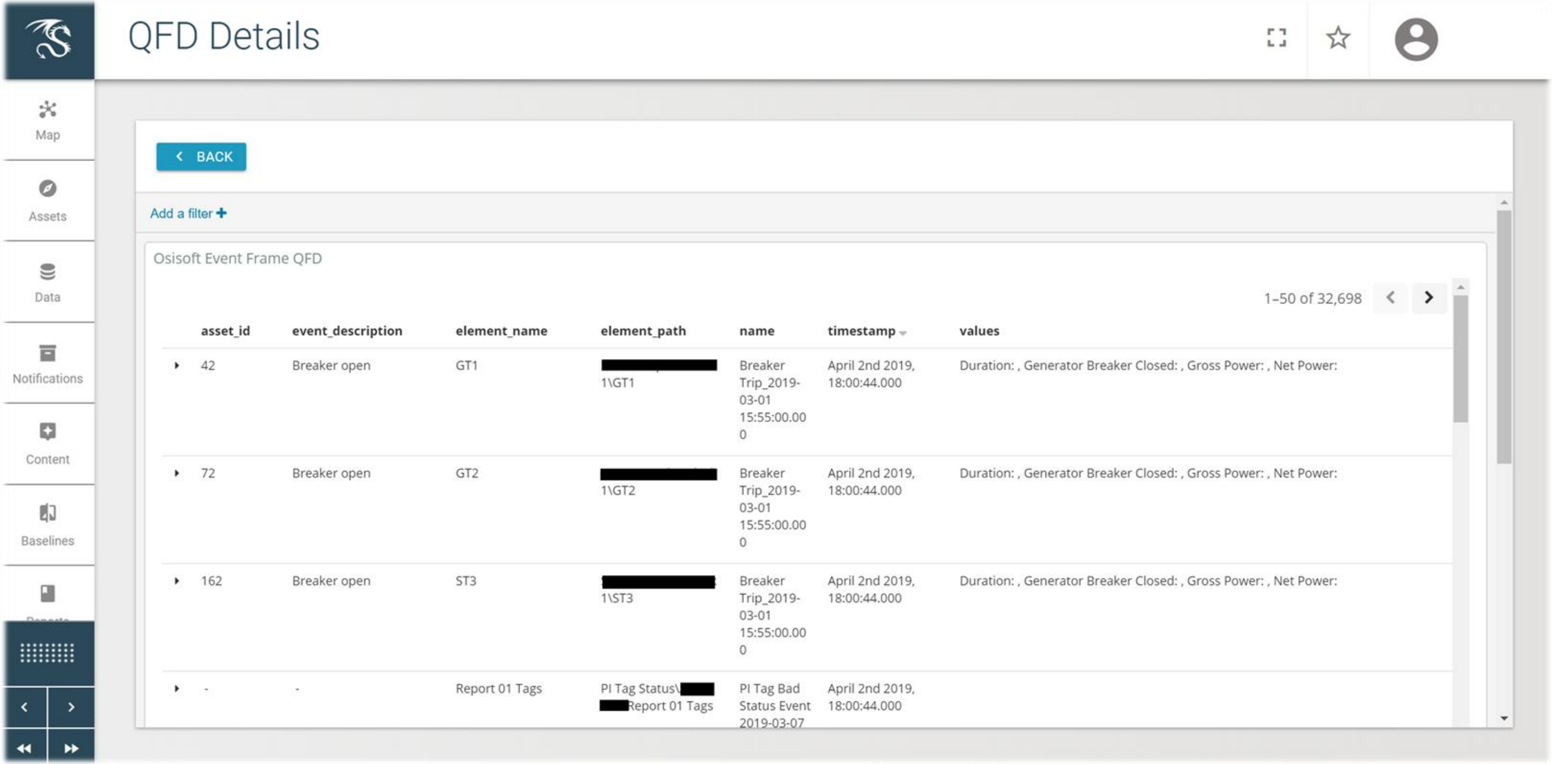
NOTIFICATIONS

Search Notifications: OSI ✕

□		Source	Summary	Detected By	F
□	▶	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...	OsiSoft EventFrame Notificatio...	0
□	▶	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...	OsiSoft EventFrame Notificatio...	0
□	▶	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...	OsiSoft EventFrame Notificatio...	0
□	▶	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...	OsiSoft EventFrame Notificatio...	0
□	▶	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...	OsiSoft EventFrame Notificatio...	0

Test

Query Focus Dataset



QFD Details

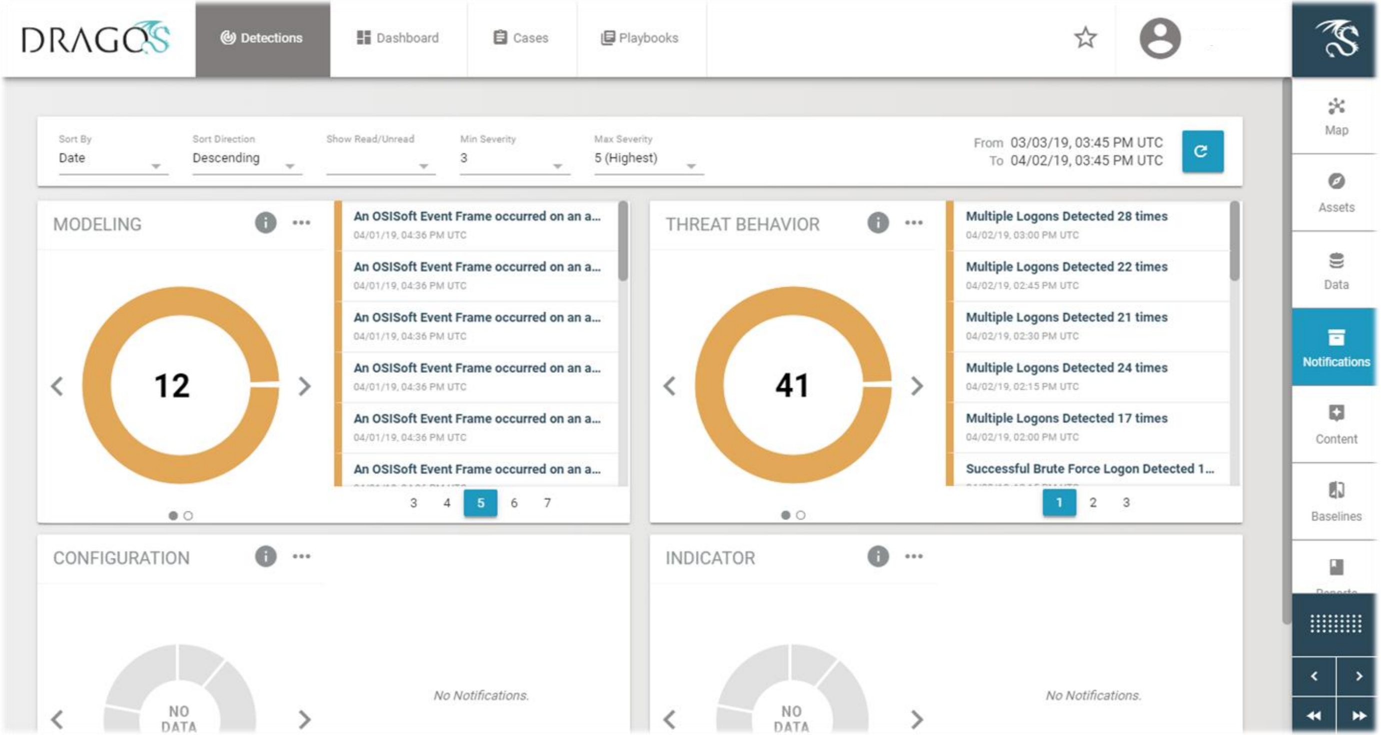
Osisoft Event Frame QFD

1–50 of 32,698

	asset_id	event_description	element_name	element_path	name	timestamp	values
▸	42	Breaker open	GT1	[redacted] 1\GT1	Breaker Trip_2019-03-01 15:55:00.000	April 2nd 2019, 18:00:44.000	Duration: , Generator Breaker Closed: , Gross Power: , Net Power:
▸	72	Breaker open	GT2	[redacted] 1\GT2	Breaker Trip_2019-03-01 15:55:00.000	April 2nd 2019, 18:00:44.000	Duration: , Generator Breaker Closed: , Gross Power: , Net Power:
▸	162	Breaker open	ST3	[redacted] 1\ST3	Breaker Trip_2019-03-01 15:55:00.000	April 2nd 2019, 18:00:44.000	Duration: , Generator Breaker Closed: , Gross Power: , Net Power:
▸	-	-	Report 01 Tags	PI Tag Status\[redacted] [redacted]Report 01 Tags	PI Tag Bad Status Event 2019-03-07	April 2nd 2019, 18:00:44.000	

Test

Detections



Sort By: Date
Sort Direction: Descending
Show Read/Unread:
Min Severity: 3
Max Severity: 5 (Highest)
From 03/03/19, 03:45 PM UTC
To 04/02/19, 03:45 PM UTC

MODELING

12

An OSISoft Event Frame occurred on an a...
04/01/19, 04:36 PM UTC

An OSISoft Event Frame occurred on an a...
04/01/19, 04:36 PM UTC

An OSISoft Event Frame occurred on an a...
04/01/19, 04:36 PM UTC

An OSISoft Event Frame occurred on an a...
04/01/19, 04:36 PM UTC

An OSISoft Event Frame occurred on an a...
04/01/19, 04:36 PM UTC

An OSISoft Event Frame occurred on an a...

3 4 5 6 7

THREAT BEHAVIOR

41

Multiple Logons Detected 28 times
04/02/19, 03:00 PM UTC

Multiple Logons Detected 22 times
04/02/19, 02:45 PM UTC

Multiple Logons Detected 21 times
04/02/19, 02:30 PM UTC

Multiple Logons Detected 24 times
04/02/19, 02:15 PM UTC

Multiple Logons Detected 17 times
04/02/19, 02:00 PM UTC

Successful Brute Force Logon Detected 1...

1 2 3

CONFIGURATION

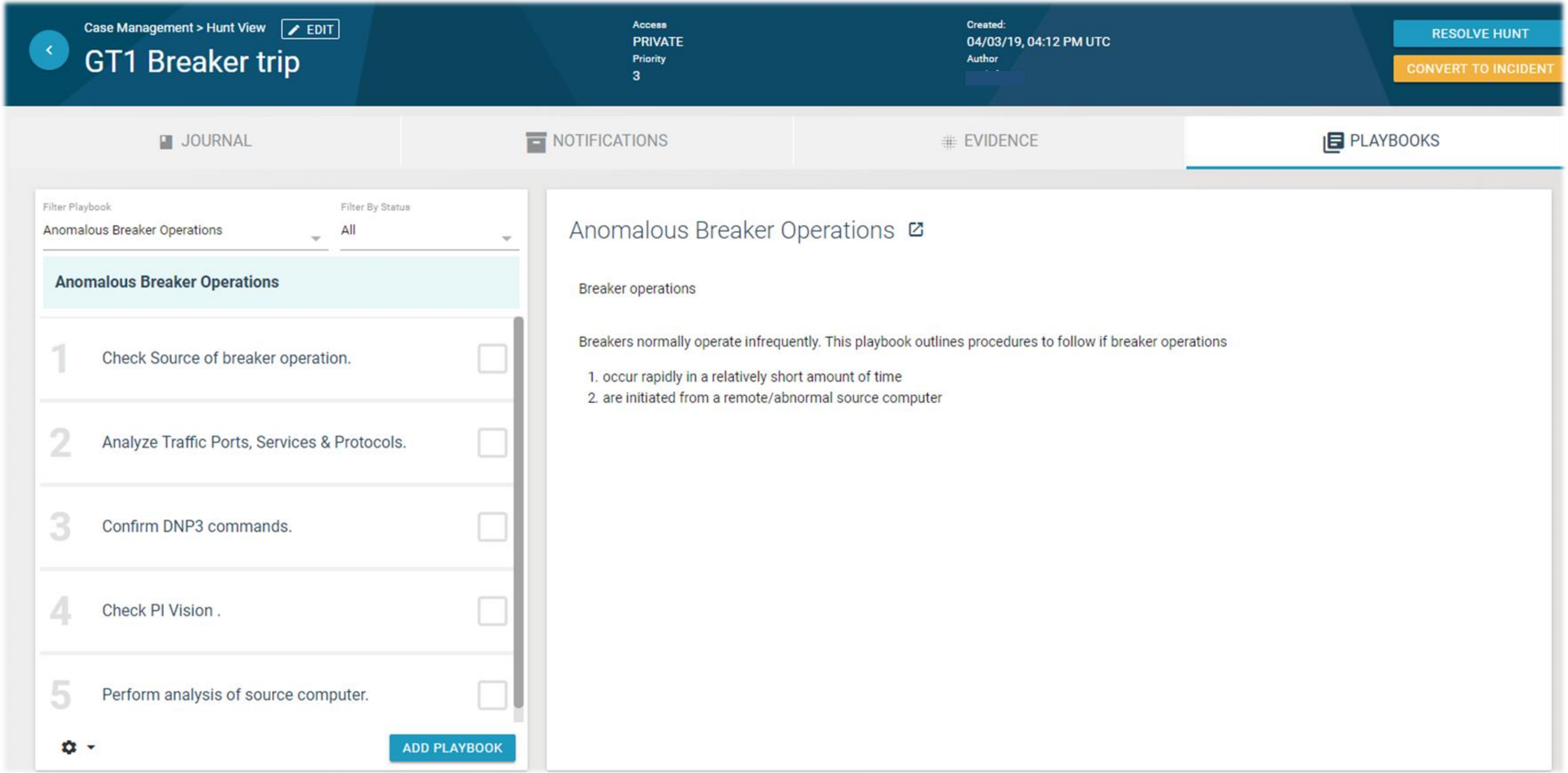
NO DATA

No Notifications.

INDICATOR

NO DATA

No Notifications.



GT1 Breaker trip

Access
PRIVATE
Priority
3

Created:
04/03/19, 04:12 PM UTC
Author
[redacted]

Filter Playbook: Anomalous Breaker Operations

Filter By Status: All

Anomalous Breaker Operations

1 Check Source of breaker operation. □

2 Analyze Traffic Ports, Services & Protocols. □

3 Confirm DNP3 commands. □

4 Check PI Vision . □

5 Perform analysis of source computer. □

Anomalous Breaker Operations

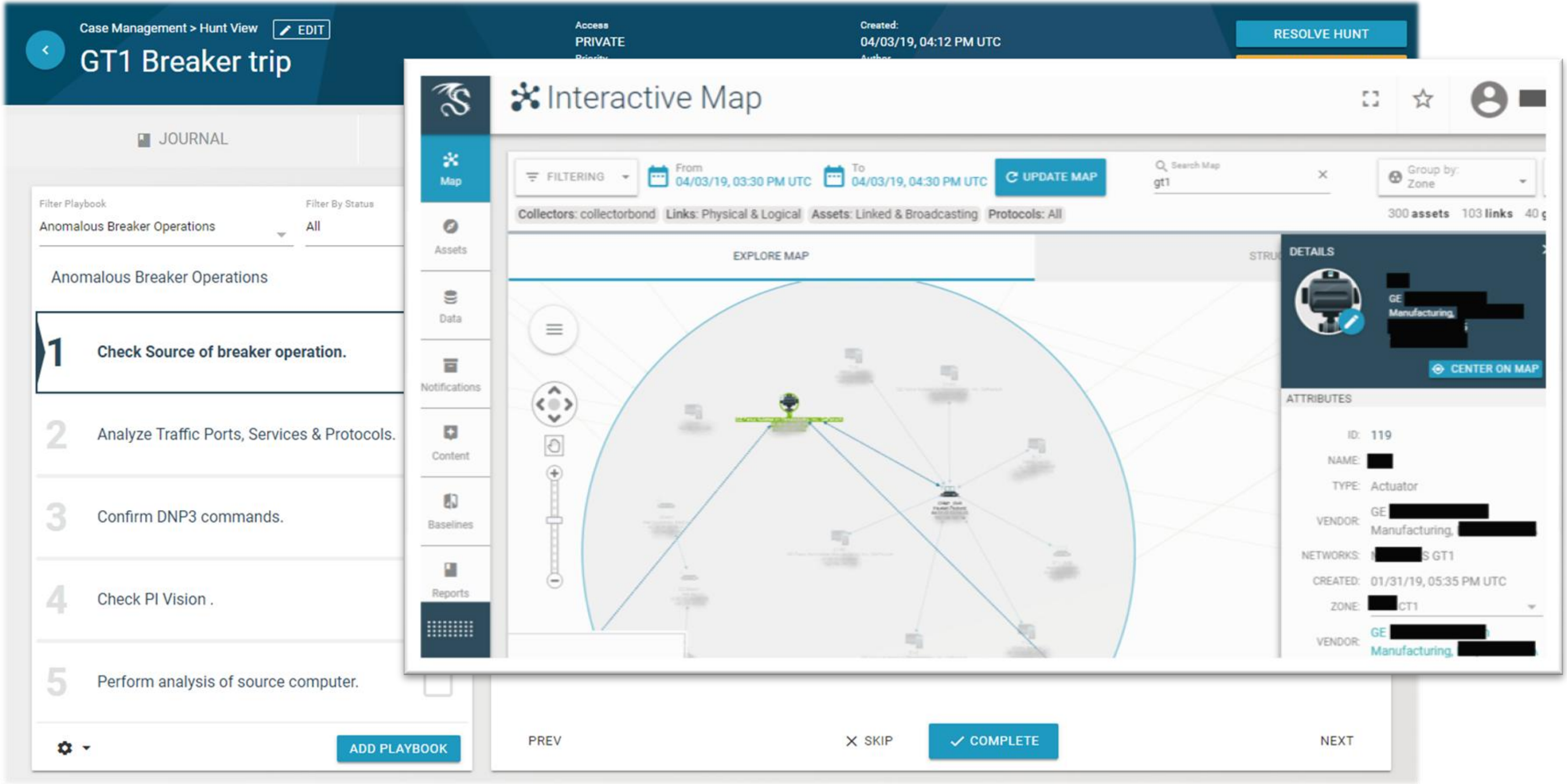
Breaker operations

Breakers normally operate infrequently. This playbook outlines procedures to follow if breaker operations

1. occur rapidly in a relatively short amount of time
2. are initiated from a remote/abnormal source computer

Start Test:

Breaker Trips
Event Frame Sent



Case Management > Hunt View

GT1 Breaker trip

Access: PRIVATE

Created: 04/03/19, 04:12 PM UTC

Filter Playbook: Anomalous Breaker Operations

Filter By Status: All

Anomalous Breaker Operations

1. Check Source of breaker operation.
2. Analyze Traffic Ports, Services & Protocols.
3. Confirm DNP3 commands.
4. Check PI Vision .
5. Perform analysis of source computer.

Interactive Map

FILTERING

From: 04/03/19, 03:30 PM UTC

To: 04/03/19, 04:30 PM UTC

Search Map: gt1

Group by: Zone

Collectors: collectorbond | Links: Physical & Logical | Assets: Linked & Broadcasting | Protocols: All

300 assets 103 links 40 g

DETAILS

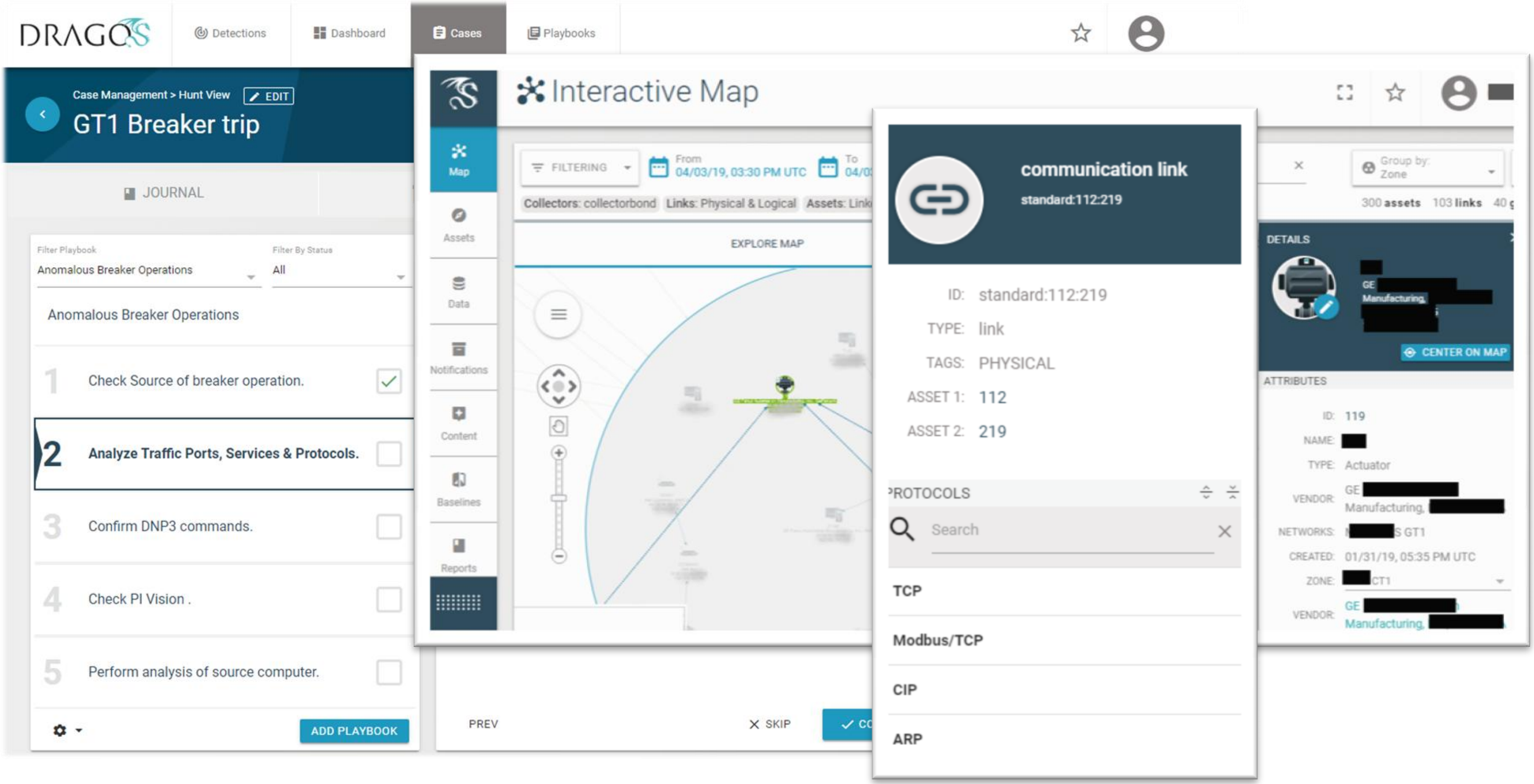
[redacted]

GE [redacted] Manufacturing, [redacted]

[redacted]

ATTRIBUTES

ID:	119
NAME:	[redacted]
TYPE:	Actuator
VENDOR:	GE [redacted] Manufacturing, [redacted]
NETWORKS:	[redacted] S GT1
CREATED:	01/31/19, 05:35 PM UTC
ZONE:	[redacted] CT1
VENDOR:	GE [redacted] Manufacturing, [redacted]



Case Management > Hunt View EDIT

GT1 Breaker trip

Filter Playbook: Anomalous Breaker Operations
Filter By Status: All

Anomalous Breaker Operations

1 Check Source of breaker operation. ☑

2 Analyze Traffic Ports, Services & Protocols. □

3 Confirm DNP3 commands. □

4 Check PI Vision . □

5 Perform analysis of source computer. □

Interactive Map

From 04/03/19, 03:30 PM UTC To 04/0

Collectors: collectorbond Links: Physical & Logical Assets: Link

communication link
standard:112:219

ID: standard:112:219
TYPE: link
TAGS: PHYSICAL
ASSET 1: 112
ASSET 2: 219

PROTOCOLS

TCP

Modbus/TCP

CIP

ARP

Group by: Zone

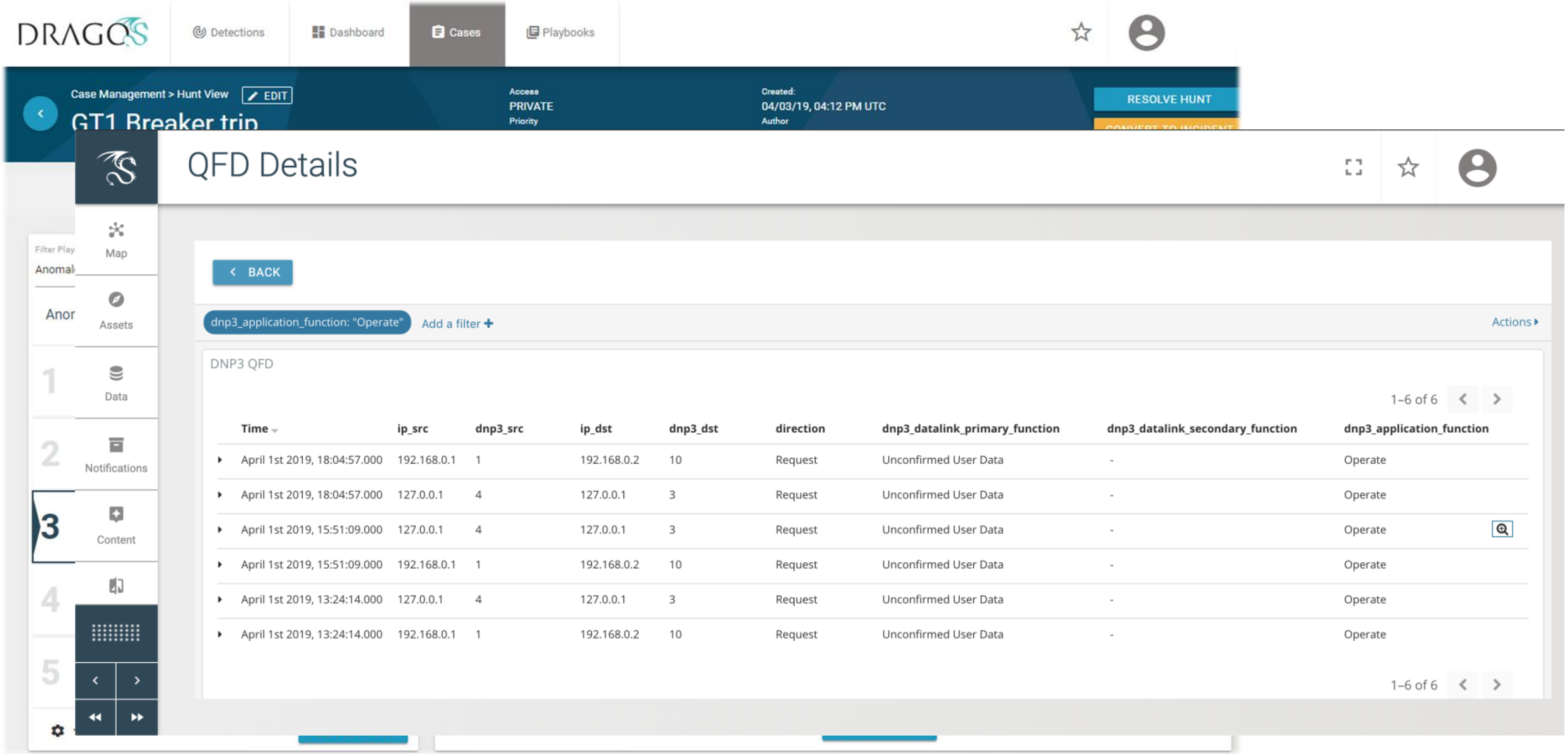
300 assets 103 links 40 g

DETAILS

[redacted]
GE [redacted]
Manufacturing, [redacted]
[redacted]

ATTRIBUTES

ID: 119
NAME: [redacted]
TYPE: Actuator
VENDOR: GE [redacted] Manufacturing, [redacted]
NETWORKS: [redacted]S GT1
CREATED: 01/31/19, 05:35 PM UTC
ZONE: [redacted]CT1
VENDOR: GE [redacted] Manufacturing, [redacted]



GT1 Breaker trip

Access
PRIVATE
Priority

Created:
04/03/19, 04:12 PM UTC
Author

QFD Details

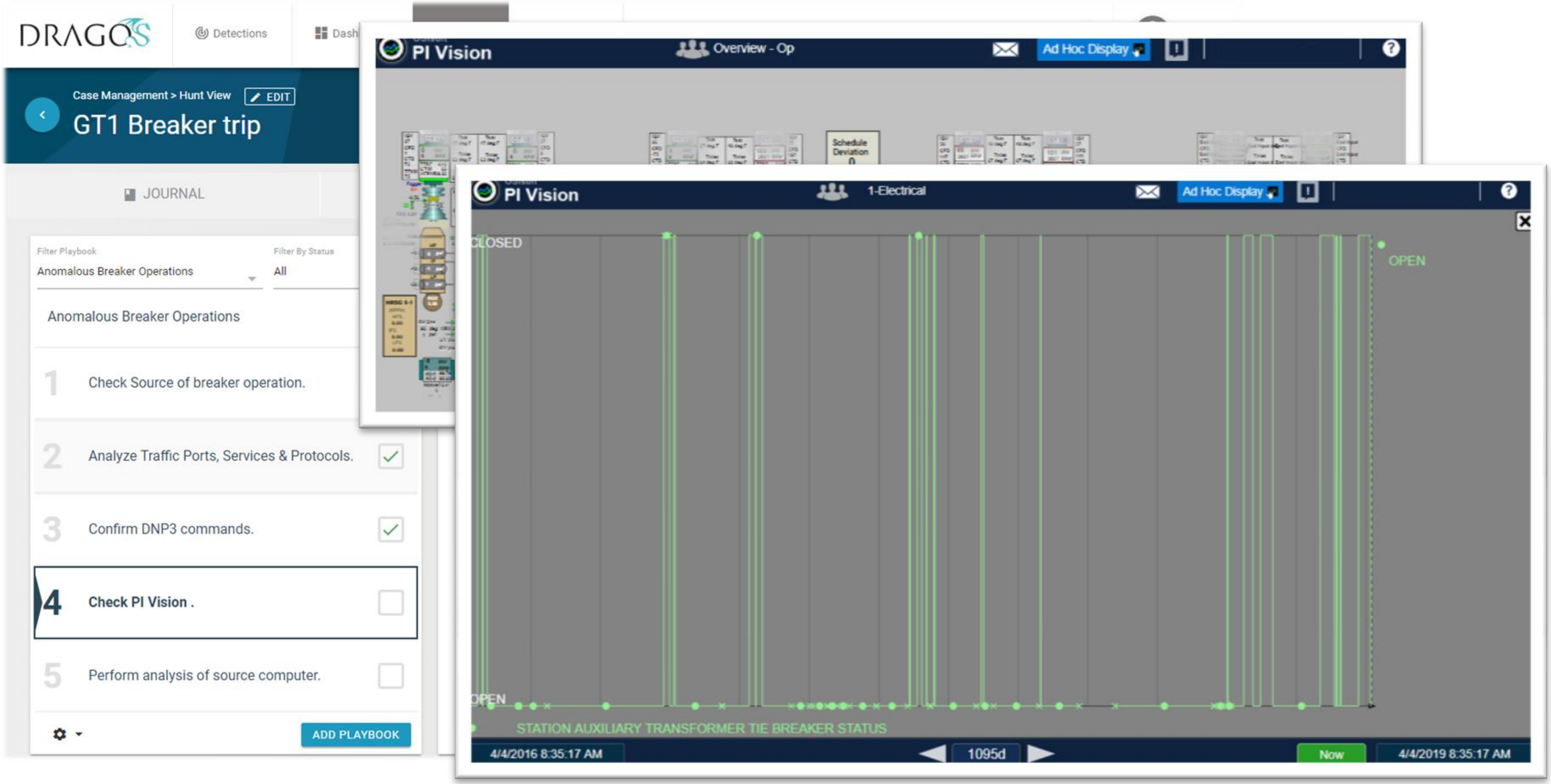
dnp3_application_function: "Operate"

DNP3 QFD

1–6 of 6

	Time	ip_src	dnp3_src	ip_dst	dnp3_dst	direction	dnp3_datalink_primary_function	dnp3_datalink_secondary_function	dnp3_application_function
▸	April 1st 2019, 18:04:57.000	192.168.0.1	1	192.168.0.2	10	Request	Unconfirmed User Data	-	Operate
▸	April 1st 2019, 18:04:57.000	127.0.0.1	4	127.0.0.1	3	Request	Unconfirmed User Data	-	Operate
▸	April 1st 2019, 15:51:09.000	127.0.0.1	4	127.0.0.1	3	Request	Unconfirmed User Data	-	Operate
▸	April 1st 2019, 15:51:09.000	192.168.0.1	1	192.168.0.2	10	Request	Unconfirmed User Data	-	Operate
▸	April 1st 2019, 13:24:14.000	127.0.0.1	4	127.0.0.1	3	Request	Unconfirmed User Data	-	Operate
▸	April 1st 2019, 13:24:14.000	192.168.0.1	1	192.168.0.2	10	Request	Unconfirmed User Data	-	Operate

1–6 of 6



Case Management > Hunt View EDIT

GT1 Breaker trip

Filter Playbook: Anomalous Breaker Operations

Filter By Status: All

Anomalous Breaker Operations

1 Check Source of breaker operation.

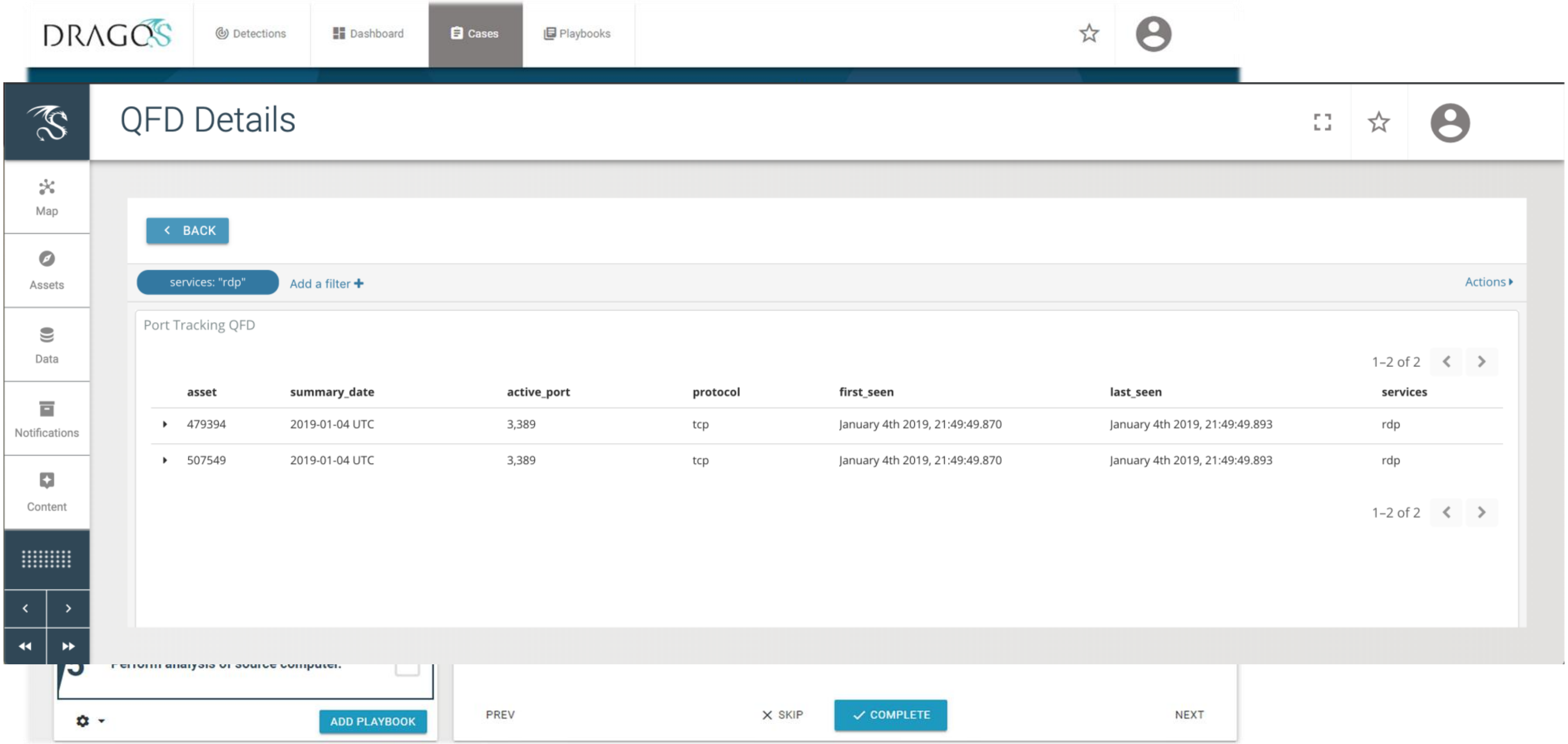
2 Analyze Traffic Ports, Services & Protocols. ☑

3 Confirm DNP3 commands. ☑

4 **Check PI Vision .** □

5 Perform analysis of source computer. □

ADD PLAYBOOK



QFD Details

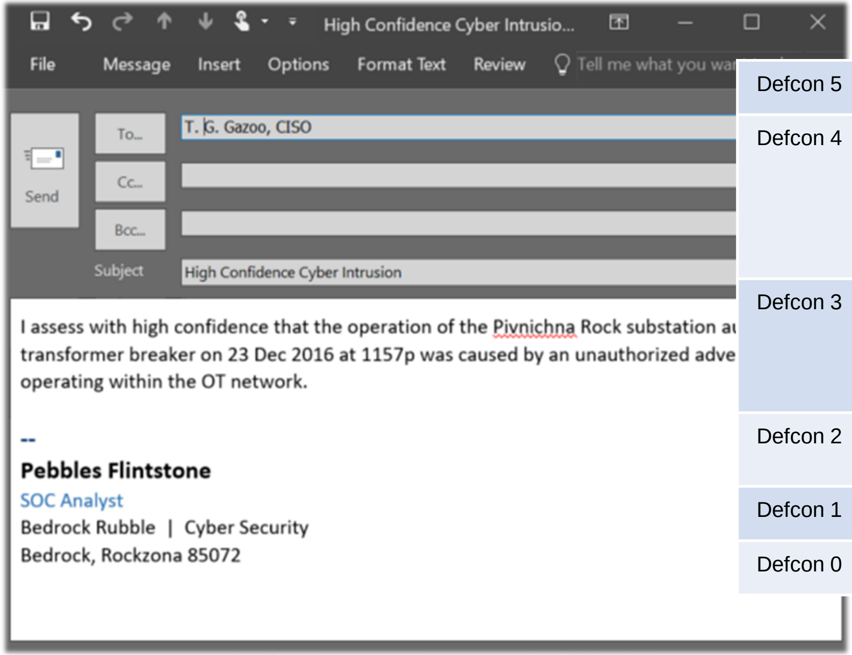
Port Tracking QFD

1–2 of 2

asset	summary_date	active_port	protocol	first_seen	last_seen	services
479394	2019-01-04 UTC	3,389	tcp	January 4th 2019, 21:49:49.870	January 4th 2019, 21:49:49.893	rdp
507549	2019-01-04 UTC	3,389	tcp	January 4th 2019, 21:49:49.870	January 4th 2019, 21:49:49.893	rdp

1–2 of 2

Quality of the Assessment (simulated) drives appropriate response actions



To: T. G. Gazoo, CISO

Subject: High Confidence Cyber Intrusion

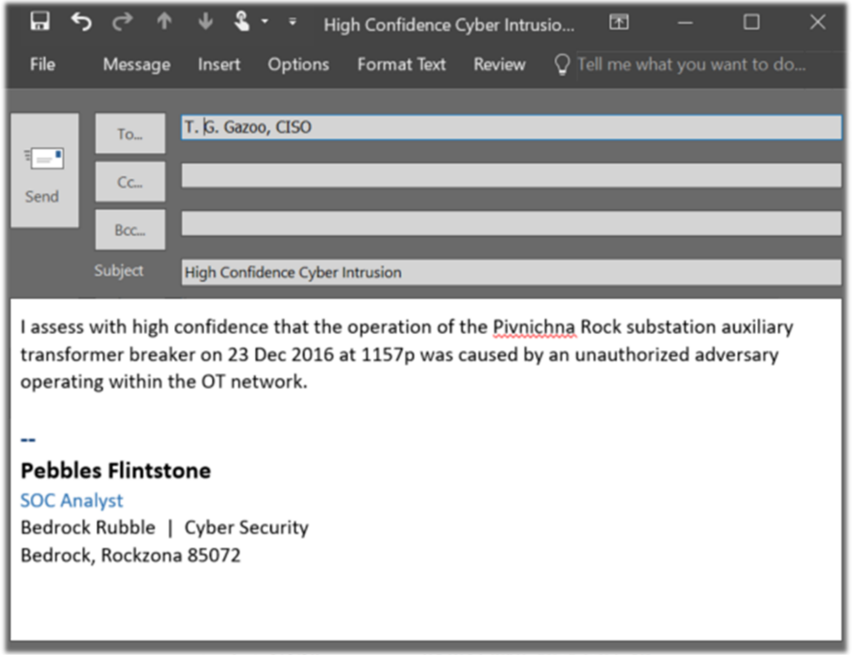
I assess with high confidence that the operation of the Pivnichna Rock substation a transformer breaker on 23 Dec 2016 at 1157p was caused by an unauthorized adve operating within the OT network.

--

Pebbles Flintstone
SOC Analyst
Bedrock Rubble | Cyber Security
Bedrock, Rockzona 85072

Defcon 5	Normal Operations – all connections active through firewalls
Defcon 4	Add email content filtering Additional web proxy filtering/Only critical web use Reduce remote access to OT zones (vendors or employees) Disable non-critical external access Increase Geo-IP blocking
Defcon 3	Strict email sanitization (reduce use, block attachments, TXT only) Limit remote access to corp Disable remote access to OT zones (vendors or employees) Reduce public internet surface area
Defcon 2	Unplug all OT network connections Disable all corp remote access
Defcon 1	Full internet disconnect
Defcon 0	Go home, hug kids, grab bug-out bag

Quality of the Assessment (simulated) drives appropriate response actions



To: T. G. Gazoo, CISO

Subject: High Confidence Cyber Intrusion

I assess with high confidence that the operation of the Pivnichna Rock substation auxiliary transformer breaker on 23 Dec 2016 at 1157p was caused by an unauthorized adversary operating within the OT network.

--

Pebbles Flintstone

SOC Analyst

Bedrock Rubble | Cyber Security

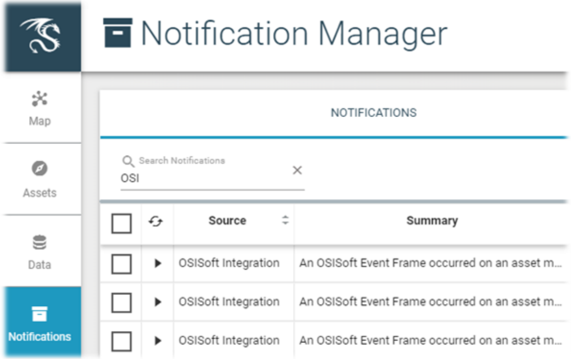
Bedrock, Rockzona 85072

NEIGHBORHOOD KEEPER
DRAGOS
STEP 01
STEP 03
Community partners (E-ISAC, INL, & opt-in Dragos Platform customers) share and receive threat insights
STEP 04
Dragos' intelligence team creates threat analytics based on behaviors and methods of ICS adversaries
STEP 05
Analytics run at sites; if threats detected, analytic outputs (e.g., metadata: "analytic 3 alerted at 2:20pm") shared to Neighborhood Keeper
STEP 06
New threats, trends, and adversary campaigns revealed from analytics help participants gain insights and prioritize defenses
E-ISAC
INL
E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER
U.S. DEPARTMENT OF HOMELAND SECURITY
CISA
CYBER+INFRASTRUCTURE

Solution, Plans, Future

SRP

Enhance Cyber Threat detection with PI data



Notification Manager

NOTIFICATIONS

Search Notifications: OSI

□		Source	Summary
□	▶	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...
□	▶	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...
□	▶	OSISoft Integration	An OSISoft Event Frame occurred on an asset m...

CHALLENGE

1. Eliminate threat activity as direct cause of operational outages
2. Improve detection of adversary tradecraft targeting OT
3. Provide data supporting fast & accurate Incident Response

SOLUTION

Integrate PI data with the Threat detection platform

- PI Event Frames notify on specific events
- Dragos Platform correlates PI data with network and endpoint data.

RESULTS

First (small) test has proven that this integration can add value

- Were able to launch an investigation based on operational events
- Provided data that allowed the analyst to make better assessments

Future Use Cases

Safety

- Can PI + Dragos identify unauthorized entry into a substation?

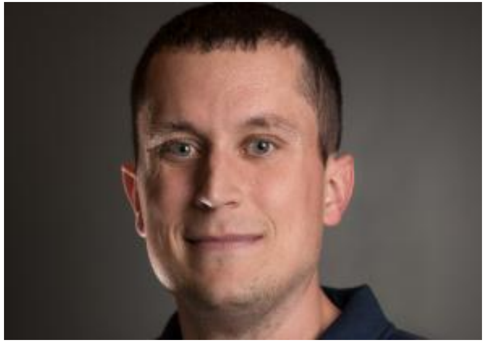
Contract Compliance

- Can PI + Dragos assure outside contractors are operating properly?

Cyber Attack

- Can PI + Dragos detect abnormal load shedding events from substations, meters, or solar inverters?

Contact



- Dan Gunter
- Principal Threat Analyst
- Dragos
- @dan_gunter

- Mark Johnson-Barbier
- Sr. Principal Analyst
- Salt River Project
- @PulseOut101

Questions?

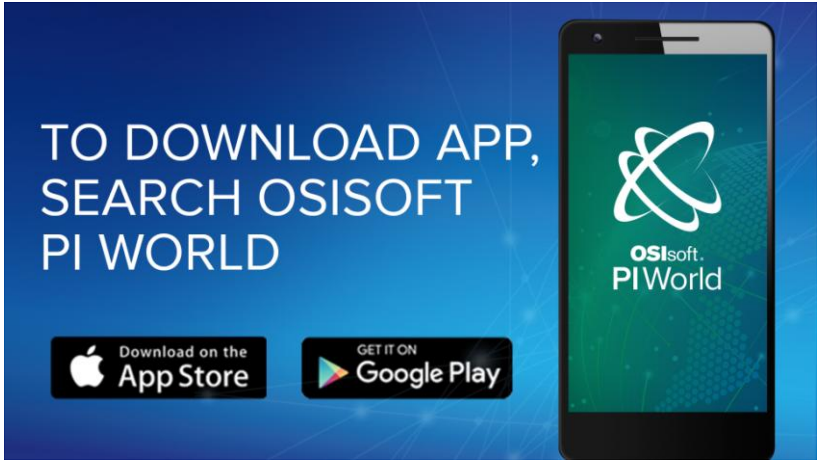
Please wait for the **microphone**

State your **name & company**

Please remember to…

Complete Survey!

Navigate to this session in mobile agenda for survey


TO DOWNLOAD APP, SEARCH OSISOFT PI WORLD
Download on the App Store
GET IT ON Google Play
OSIsoft. PI World

謝謝 KEA LEBOHA

TAPADH LEIBH 고맙습니다

DZIĘKUJĘ CI

БАЯРЛАЛАА MISAOTRA ANAO

NGIYABONGA

GRÀCIES

OBRIGADO شكرا

SALAMAT

TEŞEKKÜR EDERIM

KÖSZÖNÖM

DANKIE TERIMA KASIH DANKON TANK TAPADH LEAT

СПАСИБО

MULŢUMESC

OSIsoft PI World

РАКМЕТ СІЗГЕ

HVALA FAAFETAI

GO RAIBH MAITH AGAT

MAHADSANID

ESKERRIK ASKO

БЛАГОДАРЯ GRACIAS

THANK YOU

HVALA ХВАЛА ВАМ

TEŞEKKÜR EDERIM

ТИ БЛАГОДАРАМ

DANK JE ΕΥΧΑΡΙΣΤΩ GRATIAS TIBI

ДЗЯКУЙ

GRAZIE

TAK DANKE

AČIŪ SALAMAT MAHALO IĀ ʻOE TAKK SKAL DU HA

DI OU MÈSI

RAHMAT MERCI

FALEMINDERIT

GRAZZI ÞAKKA ÞÉR ありがとうございました

ĎAKUJEM

HATUR NUHUN РАХМАТ САҒА

SIPAS JI WERE TERIMA KASIH

MATUR NUWUN

CẢM ƠN BẠN UA TSAUG RAU KOJ

WAZVIITA

ТИ БЛАГОДАРАМ

СИПОС